REMARKS

This Amendment is submitted in response to the Official Action dated September 2, 2009. Claims 1-7, 9-11, 15-18, and 35 are amended, and claims 1-11, 15-18, 34, and 35 remain pending in this application.

Claims 4 and 10 are objected to because of informalities.

Claim 4 is amended as suggested by replacing select commas with semicolons and by insert "or" between "OCSP" and "LDAP."

Claim 10 is amended by replacing "are" with "is."

Claims 1-11, 15-18, 34, and 35 are rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

The preamble of claim 1 is amended to read "for checking validities of certificates receiving one or more certificate status queries" to clarify that the antecedent basis of "the certificates" in line 7 of claim 1 is the term "certificates" in the preamble. Claim 1 is also amended to read "a CSS cache memory." Further, claim 1 is amended to read "fetching, from a CSS configuration store, all certificate status reporting methods and communications information that are needed for retrieving, from the respective issuing CAs, a certificate status of each certificate whose status has not yet been determined" to clarify that "from a configuration store" modifies *fetching*, to clarify that the subject of the phrase "that are needed for retrieving" is the status reporting methods and communications information, and to clarify that "from the respective issuing CAs" modifies *retrieving*. Claim 1 is also amended to read "processing the certificate statuses

according to the appropriate certificate status reporting methods" to reflect that there may be more than one reporting method used. The phrase "the CSS's cache memory" in line 28 is replaced with the phrase "CSS cache memory." To clarify the wherein clause, claim 1 is amended to read "wherein the issuing CAs and connector parameters, which enable the CSS to interwork with any CAs and CA domains even though the CSS and issuing CAs may operate using dissimilar certificate practices and policies, are designated on a list of approved CAs in the CSS configuration store."

Claim 2 is amended to read "a certificate indicating a validity period is deemed to have expired if a local date and time fall outside the validity period" to clarify the limitation.

In claim 3, the phrase "the organization" in lines 8 and 9 is replaced with the phrase "the at least one organization."

Claim 4 is amended to read "adding, to the CSS configuration store" to clarify to what the component, method, and information are added.

In claim 5, the phrase "the certificate status" is replaced with "the queried certificate status."

In claim 9, the phrase "the connector allows" is replaced with "the connectors allow."

In claim 11, the phrases "the certificate" and "the approved CA" are replaced with the phrases "the certificates" and "the approved CAs," respectively. The steps following the second conditional are indented further to clearly indicate that these steps occur if the second condition is met. The phrase "the issuing CA" is replaced with the "issuing CAs."

In claim 15, the phrase "the threshold" in line 14 is replaced with "the respective thresholds," and the phrase "the status" in line 14 is replaced with "the certificate statuses."

In claim 16, the preamble now reads "[t]he method of claim 15." and the phrase "a threshold" is replaced with "the respective thresholds."

In claim 17, the preamble now reads "[t]he method of claim 16."

In claim 18, the preamble now reads "[t]he method of claim 17."

In claim 35, the phrase "that CSS" is replaced with the phrase "that other CSS."

Claims 1-11, 15, and 35 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Koehler, US Patent 6301658, in view of Barrett et al., US Patent 6581059.

All claim limitations are significant and must be given weight and effect in relation to claim patentability, see *In re Saether*, 492 F.2d 849, 852 (C.C.P.A. 1974), and if the combination fails to teach a single claim limitation, the claim cannot be obvious over the prior art, see *In re Glass*, 472 F.2d 1388, 1392 (C.C.P.A. 1973). Thus, even assuming, arguendo, that there were some motivation to combine the Koehler and Barrett as suggested by the Examiner, as must be demonstrated, the combination still falls far short of teaching the claimed invention, and therefore, claims 1-11, 15, and 35 are patentably distinct.

Notably, the claimed CSS methods create and maintain a trusted environment that allows a CSS to interoperate and interwork with all approved certificate status reporting components, CA hierarchies, stand-alone CAs, and self-signed CAs: "to interwork with

any CAs and CA domains even though the CSS and issuing CAs may operate using dissimilar certificate practices and policies." The CSS retrieves, processes, stores, and reports certificate statuses using *any reporting method*, which allows the CSS to process multiple types of certificates including those that support identification and authentication; communication; media; memory; and messaging encryption. The CSS employs a number of methods to reduce communications and processing overhead and to remove stale certificate statuses such as use-counter, time-to-live, last-accessed, and new CRL retrieval.

The Koehler verification server is simply a certificate status reporting component that off-loads CRL processing and direct CA communications for a multitude of entities requesting certificate status. The verification server retrieves, processes, stores, and reports certificate statuses derived from CRLs created by CAs within a single CA hierarchy. The CA hierarchy certificate chain is also verified to insure that retrieved CRLs are still valid. No other capability is disclosed. Interoperability and interworking are never addressed because the Koehler verification server is only intended to work within a single CA hierarchy in which the CAs use the same certificate policies and practices.

Specifically regarding claim 1, the Examiner submits that Koehler discloses that if at least one status needs to be determined, fetching information needed for retrieving a status of an authentication certificate from a respective issuing. Claim 1 requires "fetching, from a CSS configuration store, all *certificate status reporting methods* and *communications information* that are needed for retrieving, from the respective issuing CAs, a certificate status of each certificate whose status has not yet been determined."

The Applicant notes that the claimed CSS is capable of using *multiple* "certificate status reporting *methods*," for example, LDAP, OCSP, and CRLs. The verification server of Koehler only uses a single method, CRL. The Applicant notes that phrase "communications information" used in claim 1 may comprise IP addresses, SSL keys, and certificates—all the information needed to query the appropriate certificate status component. (*See* Application paragraphs 80 & 124). The Applicant submits that Koehler merely teaches that the cited CA information identifies the issuing CA—the name of the issuer—and does not indicate the specific information needed to communicate with the status reporting component. These claimed limitations allow interoperability and interworking with any CA reporting component regardless of the status reporting method and reporting component used.

The Examiner also cites to Koehler for teaching configuring connectors based on the identified information for communicating with the issuing CA and communicating with the issuing CA according to the configured connector when the status of the authentication certificate is queried. Claim 1, as amended, requires "configuring *connectors* based on the identified information for communicating with the issuing CAs" and "communicating with the issuing CAs according to the configured *connectors*." A connector or programming module is defined for each certificate status method for communication between the CSS and the issuing CA, and the appropriate connector based on the status reporting method is invoked to retrieve the status from the issuing CA. (See Application paragraph 58). The Applicant respectfully submits Koehler never discloses connectors that would allow the verification server to work concurrently with multiple certificate status reporting components. Even assuming for the sake of argument

that Koehler teaches a connector, Koehler fails to teach or imply multiply "connectors" because only one status reporting method, CRL, is used in Koehler. Again, these distinctions are important because multiply connectors allow interoperability with any CA regardless of the status reporting method used. Thus, claim 1 is patentably distinct because the combination of Koehler and Barrett fails to teach every limitation.

Claim 2 is dependent on claim 1 and, therefore, is likewise patentably distinguished for the reasons presented above.

Regarding claim 3, the Examiner submits that Koehler and Barrett disclose that the issuing CA is added to a list of approved CAs by vetting and approving the issuing CA according to predetermined business rules, and if the issuing CA is vetted and not approved, the issuing CA is added to a list of not-approved CAs in the configuration store. As the Examiner, noted Koehler does not disclose a list of approved CAs and, thus, cannot teach the claimed limitation. Further, the Applicant submits that Barrett merely discloses that "entities are allowed to define a list of identities associated with third party certification authorities that are allowed to perform the verification," but does not disclose the necessary criteria to be added to the list of approved CAs, such as the claimed "predetermined business rules, wherein the business rules include at least one rule for reviewing the acceptability of the CA's certificate policy and practices for insuring the identity of the entity requesting the certificate." The Applicant also notes that Barrett does not teach the claimed "list of not-approved CAs." Thus, claim 3 is patentably distinguished from the combination of Koehler and Barrett because the combination fails to teach every limitation.

Regarding claim 4, the Examiner asserts that the combination discloses that vetting and approving the issuing CA includes registering a representation of the CA's trusted authentication certificate with the CSS and adding a status reporting component, the status reporting method such as CRL, a time-to-live data element, and configuration information for a connector. The Applicant submits that Koehler merely discloses a timestamp that indicates when the item was last verified. The claimed "time-to-live data element," however, indicates when a stored certificate status needs to be removed or updated, not when it was last verified. Further, Koehler does not disclose storing in the configuration store a status reporting component, status reporting method, or configuration information. Thus, claim 4 is also patentably distinguished because the combination fails to teach every claim limitation.

Claim 5, as amended, reads "checking . . . that the time-to-live data element and use-counter values are within a threshold" and "if any . . . time-to-live data element, or use-counter values are unacceptable, clearing the CSS cache memory." The Koehler timestamp is not equivalent to the time-to-live data element. The time-to-live element specifies the period over which the cached status can be reused, normally less than 5 minutes, while the Koehler timestamp indicates when a cached item, CRL or certificate, was last authenticated. The Koehler timestamp is also used to update and replace cache entries, not to clear the cache memory. Additionally, the Applicant submits that Koehler does not disclose a use-counter value that is determined by the number of times the certificate's status is checked. (See paragraph 38.) Thus, claim 5 is patentably distinguished because the cited combination fails to teach every limitation.

Claim 6, as amended, states "according to a publication schedule of the issuing CA, wherein the CSS retrieves the CRL from a certificate status reporting component listed in the CSS configuration store." The Applicant submits that although Koehler discloses that the verification server maintains cache entries for CRLs, Koehler does not disclose retrieving the CRLs according to the publication schedule. Claim 6 is thus patentably distinguished from the asserted combination because the combination fails to teach every limitation of the claim.

In claim 7, a ΔCRL is indicated as a reporting method: "wherein the certificate status reporting method is indicated to be a ΔCRL." Koehler does not teach ΔCRL retrieval or processing, which is distinguished from complete CRL retrieval and processing as used in Koehler. Thus, claim 7 is patentably distinguished.

Regarding claim 8, the Applicant submits that Koehler discloses a plurality of clients making certificate status requests, which is distinguished from the claimed "plurality of connectors" used to communicate and retrieve certificate statuses from multiple approved certificate status reporting components, CA hierarchies, and standalone CAs. In fact, Koehler does not specifically disclose how the verification server communicates with the CAs within the single CA hierarchy.

Claim 9 states "connectors allow more than one certificate status request to be chained together in a single communicating step between the CSS and the issuing CA." The Applicant submits that although Koehler discloses that the verification sever receives a plurality of requests from clients to authenticate certificates issued by a hierarchy of certification authorities, Koehler does not teach retrieving a plurality of CRLs or real-

time certificate statuses in one communications step. Thus, claim 9 is patentably distinguished.

Regarding claim 10, the Applicant submits that Koehler discloses that the cache entry is updated if the timestamp is out of date or issues an invalid response if the certificate has expired. The Applicant notes, however, that Koehler does not disclose removing the entry from a configuration store if the cached status has expired.

Claim 11, as amended, requires "obtaining the communications information, certificate status types, and retrieval methods from the CSS configuration store." The Applicant again notes that the phrase "communications information" comprises the information necessary to query the status reporting component, but the CA information of Koehler simply names of the issuer and does not include communication parameters. Further, the Applicant notes that CSS obtains the certificate status type from the CSS configuration store. Because the verification server in Koehler only uses CRLs, this limitation is not necessary and is not disclosed in Koehler. Unlike the Koehler verification server, the claimed CSS can use multiple certificate status types, for example, LDAP, OCSP, and CRLs. The Applicant also notes that claim 11 requires certain action "if . . . local time is greater than a next scheduled publication time for the CRL." Koehler discusses timestamps associated with cache entries, but does not discuss CRL publication schedules. Further, claim 11, as amended, requires "creating connectors and composing certificate status requests according to the certificate status type," but Applicant again submits that Koehler does not teach a connector as defined in the application, use of multiple connectors, or configuring connectors according to the communication information because only one status reporting method, CRL, is used in Koehler.

Additionally, claim 11 states "associating, with the interpreted retrieved certificate statuses, time-to-live values representing periods specified by the respective CSS policies for the certificate status types." The Applicant again submits that the Koehler timestamp is not equivalent to the time-to-live value. Therefore, claim 11 is patentably distinguished from the cited combination because it fails to teach every limitation.

Regarding claim 15, the Applicant again asserts that the claimed time-to-live value is distinguished from the Koehler timestamp; that Koehler does not disclose a use-counter value; and that Koehler does not disclose retrieving CRLs based on the publication schedule. Because the cited combination fails to teach every limitation, claim 15 is patentably distinguished.

Regarding claim 35, the Examiner submits that Koehler and Barrett disclose that any CSS can query any other CSS for the certificate status if that CSS is designated as an approved status reporting component for the CA. The Applicant respectfully disagrees because Koehler discloses a verification server querying a certificate repository, but does not disclose a verification server querying other verification servers. (See Koehler Figure 2.) Second, Barrett discloses a list of certification authorities (CAs) that are allowed to perform verification, but does not teach listing any specifics about the CAs such as designated status reporting components. Claim 35 is patentably distinguished.

Claims 16-18 and 34 are rejected under 35 U.S.C. § 103(a) as being unpatentable over Koehler in view of Barrett as applied to claim 15 above, and further in view of Konheim, US Patent 4264782.

Claim 16 is dependent on claim 15 and, therefore, is likewise patentably distinguished for the reasons presented above. Further, claim 16 states that the CSS cache memory is cleared when the use-counter value exceeds its respective threshold, but neither Koehler nor Konheim disclose this limitation.

Regarding claim 17, the Examiner submits that Koehler, Barrett, and Konheim disclose that a status last-accessed data element is added to the cache memory, and the status last-accessed data element in conjunction with the status use-counter data element enable determination of an activity level of the certificate's status. The Applicant submits, however, that Konheim uses a counter to prevent retransmission of a previously validated message, not to determine the activity level of the certificate's status. The claimed CSS employs the use-counter value to allow reuse of real-time certificate statuses until the value exceeds the threshold. Therefore, claim 17 is patentably distinguished.

Regarding claim 18, the Examiner asserts that Koehler, Barrett, and Konheim disclose that when a request is made to the CSS to retrieve a status of a new certificate and the cache memory has reached an allocated buffer size limit, the CSS searches the cache memory for a least-accessed data element indicating an oldest date and clears the respective cache memory entry. The Applicant notes that although the Koehler verification server overwrites cache entries with updated CRLs, certificates, and timestamps, Koehler does not disclose a method to free up more cache if needed. The claimed CSS frees up all cache memory associated with stale certificate statuses when certificates expire or the cleanup process determines that one of the certificate status use control values exceeds its threshold.

Regarding claim 34, the Applicant submits that Koehler, Barrett, and Konheim disclose a verification server that merely replaces old items, CRLs, and CA certificates

with updated. Conversely, the claimed CSS uses multiple use controls that determine when certificate statuses need to be removed from cache including certificate expiration, time-to-live, use-counter, and last-accessed data elements. The CSS removes all identified stale certificate statuses from cache anytime space is needed.

* * * * *

In light of the foregoing amendments and argument, Applicant asserts that claims are now in condition for allowance. As the amendments do not introduce any new issues into the present application, entry and allowance are believed to be appropriate.

Respectfully submitted,

Royal W. Craig
Attorney for Applicant
Reg. No. 34,145

Royal W. Craig
Ober, Kaler, Grimes & Shriver
120 East Baltimore Street, Suite 800
Baltimore, MD 21202-1643
Telephone: (410) 347-7303